WE CLAIM:

1. A computer program product for controlling a computer to scan data accessible via an internet link for malware, said computer program product comprising:

(i) address identifying code operable to identify within currently held data at least one internet address associated with said currently held data;

(ii) retrieving code operable to retrieve via said internet link addressed data corresponding to said at least one internet address; and

(iii) scanning code operable to scan said addressed data for malware.

2. A computer program product as claimed in claim 1, further comprising storing code operable to store result data identifying at least addressed data in which malware was not found.

3. A computer program product as claimed in claim 1, wherein said address identifying code is operable to search within said currently held data for string data having a format matching a pointer to an internet address.

4. A computer program product as claimed in claim 1, wherein said currently held data includes received e-mail messages.

5. A computer program product as claimed in claim 1, wherein said scanning code is operable to seek to detect within said addressed data one or more of:

computer viruses;
worms;
Trojans;
banned computer programs;
banned words; or
banned images.

6. A computer program product as claimed in claim 1, wherein said computer is a firewall computer via which internet traffic is passed to a local computer network.

7. A computer program product as claimed in claim 1, wherein said addressed data is cached when it has been retrieved.

8. A computer program product as claimed in claim 1, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

9. A computer program product as claimed in claim 1, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(iv) blocking internet access by a computer detected to be seeking to access said at least one internet address.

10. A method of scanning data accessible via an internet link for malware, said method comprising the steps of:

(i) identifying within currently held data at least one internet address associated with said currently held data;

(ii) retrieving via said internet link addressed data corresponding to said at least one internet address; and

(iii) scanning said addressed data for malware.

11. A method as claimed in claim 10, further comprising storing result data identifying at least addressed data in which malware was not found.

12. A method as claimed in claim 10, wherein said step of identifying includes searching within said currently held data for string data having a format matching a pointer to an internet address.

19. Apparatus for scanning data accessible via an internet link for malware, said apparatus comprising:

(i) address identifying logic operable to identify within currently held data at least one internet address associated with said currently held data;

(ii) retrieving logic operable to retrieve via said internet link addressed data corresponding to said at least one internet address; and

(iii) scanning logic operable to scan said addressed data for malware.

20. Apparatus as claimed in claim 19, further comprising storing logic operable to store result data identifying at least addressed data in which malware was not found.

21. Apparatus as claimed in claim 19, wherein said address identifying logic is operable to search within said currently held data for string data having a format matching a pointer to an internet address.

22. Apparatus as claimed in claim 19, wherein said currently held data includes received e-mail messages.

23. Apparatus as claimed in claim 19, wherein said scanning logic is operable to seek to detect within said addressed data one or more of:

computer viruses;

worms;

Trojans;

banned computer programs;

banned words; or

banned images.

24. Apparatus as claimed in claim 19, wherein said computer is a firewall computer via which internet traffic is passed to a local computer network.

25. Apparatus as claimed in claim 19, wherein said addressed data is cached when it has been retrieved.

26. Apparatus as claimed in claim 19, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

27. Apparatus as claimed in claim 19, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(v) blocking internet access by a computer detected to be seeking to access said at least one internet address.